UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

KELLEY WHALEN, on behalf of herself and all others similarly situated, **Plaintiff** **v.** **SUNRISE MEDICAL LABORATORIES, INC.,** **Defendants.**	**CASE NO.:** 19-cv-4378 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Kelley Whalen ("Plaintiff"), individually and on behalf of those similarly situated, brings this class action lawsuit against Sunrise Medical Laboratories, Inc. ("Sunrise") ("Defendants") based upon personal knowledge as to herself, and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for failing to properly secure and safeguard protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, financial information, and other personally identifiable information (collectively, "PII")[1]; failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members (defined below) that the integrity of their PII had been compromised; and failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members of the nature and scope of the PII that was exposed.

[1] PII includes, but is not limited to, protected health information as defined by the Health Insurance Portability and Accountability Act, medical information, and other personally identifiable information including, without limitation to, names, health plan identification numbers, social security numbers, financial information, dates of birth, gender, address, health plan names, health plan eligibility dates, insurance types and coverage information.

2. On July 15, 2019, Sunrise publicly announced that its billing collections vendor, AMCA, had been breached exposing the PII of approximately 427,000 Sunrise customers whose data was stored on the affected system. Sunrise had provided its customer PII as part of its bill collection protocols. According to Sunrise, the PII consisted of customers' "names, addresses, phone numbers, dates of birth, dates of service, balance information, credit card or banking information, and treatment provider information" (the "Data Breach").[2] The Data Breach occurred between August 1, 2018 and March 30, 2019.

3. AMCA became aware that patients' PII was compromised on March 21, 2019, but did not inform Sunrise of the Data Breach until May 2019. Sunrise waited another two months to notify its patients, preventing Plaintiff and the proposed Class from taking steps to prevent the further actual and potential misuse of their PII.

4. To date, Sunrise has not disclosed the full extent and nature of the Data Breach, nor offered anything to its patients to address and compensate for the harm they have suffered.

5. This Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Patient PII.

6. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to follow reasonable practices in hiring third party vendors who would be responsible for PII; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely

[2] Sunrise Medical Laboratories, Inc. Notifies Patients of Data Security Incident, available at https://www.prnewswire.com/news-releases/sunrise-medical-laboratories-inc-notifies-patients-of-data-security-incident-300885210.html (last visited July 25, 2019).

detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

7. As a result of Defendant's failure to implement and follow basic security procedures, patient PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

8. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, invasion of privacy, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence, and violation of New York's Information Security Breach and Notification Act, and seeks to compel Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices to safeguard patient PII that remains in their custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

9. Plaintiff Kelley Whalen is a resident of New York and a Sunrise Medical patient. Plaintiff received a letter from Sunrise dated July 15, 2019 with the subject line "Data Security Incident" indicating that her PII had been improperly exposed.

10. As a result of the Data Breach, Defendant's failure to prevent the Data Breach, and Defendant's failure to timely disclose the Data Breach, Plaintiff will continue to be at heightened risk for medical fraud, financial fraud, and identity theft along with their attendant damages for years to come.

11. Sunrise Medical Laboratories, Inc. is a New York company headquartered at 250 Miller Place, Hicksville, NY 11801. Sunrise serves patients in New York, New Jersey, Maryland, Virginia, West Virginia, Washington D.C., and Connecticut.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). On information and belief, the amount in controversy exceeds $5 million, exclusive of interest and costs. There are approximately 427,000 million putative class members, at least some of whom have a different citizenship from Defendant.

13. This Court has jurisdiction over Defendant because it is incorporated in New York and its principal place of business is in this District, and a substantial part of the conduct alleged in this Complaint occurred in, was directed to, and/or emanated in part from this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Venue is also proper because Defendant is incorporated in New York and its principal place of business is in this District.

STATEMENT OF FACTS

A. *The Data Breach*

15. On July 15, 2019, Sunrise announced that the highly sensitive PII of approximately 427,000 of its patients had been improperly exposed over a seven-month period. The breach occurred on the system of Sunrise's billing collections vendor, AMCA. According to the announcement, a data security incident occurred affecting an AMCA database containing information for some Sunrise patients. According to Sunrise, the Data Breach exposed at least some

of its customers "names, addresses, phone numbers, dates of birth, dates of service, balance information, credit card or banking information, and treatment provider information."[3]

16. According to the July 15, 2019, announcement:

> Sunrise Medical Laboratories, Inc. ("SML") has been informed by Retrieval Masters Creditors Bureau d/b/a American Medical Collection Agency ("AMCA") of a data security incident involving the AMCA payment website. AMCA is an independent collection agency that SML and many other entities used for debt collection. The incident is limited to AMCA's systems. The security of SML's systems was not affected by this incident.
>
> According to AMCA, on March 21, 2019, AMCA became aware of facts indicating there had been a data security incident. After conducting an investigation, in May of 2019, AMCA notified SML about the incident and informed SML that an AMCA database containing information for some SML patients had been affected. However, at the time of AMCA's initial notification, AMCA did not provide SML with enough information for SML to identify potentially affected patients or confirm the nature of patient information potentially involved in the incident, and SML's investigation is on-going. Based on the information provided by AMCA, the following information belonging to SML patients may have been affected by the incident: patient names, addresses, phone numbers, dates of birth, dates of service, balance information, credit card or banking information and treatment provider information. AMCA has advised SML that its patients' social security numbers were not involved in the incident. SML does not provide AMCA healthcare records such as laboratory results and clinical history.
>
> In response to the breach, AMCA sent notification letters to approximately 15,000 SML patients informing them that their names, addresses, phone numbers, dates of birth, dates of service, balance information, credit card or banking information and treatment provider information may have been impacted. In addition, based on the investigation and the information provided by AMCA, SML estimates that approximately another 412,000 patients may have had their names, addresses, phone numbers, dates of birth, dates of service, balance information and treatment provider information impacted by this incident. For these patients, credit card and banking information is not impacted. The impact of this incident is limited to patients whose accounts were referred for debt collection and who reside in the United States.
>
> Individuals with questions about this incident or questions about precautionary steps they can take may call 833-300-6926 for additional information.

[3] Sunrise Medical Laboratories, Inc. Notifies Patients of Data Security Incident, available at https://www.prnewswire.com/news-releases/sunrise-medical-laboratories-inc-notifies-patients-of-data-security-incident-300885210.html (last visited July 25, 2019).

> SML takes the security of its patients' information very seriously, including the security of data handled by vendors. As a result of the investigation, SML is no longer using AMCA for collection efforts.
>
> The privacy and protection of patient information is a top priority. SML greatly appreciates the patience and loyalty of its patients as it works to respond to this incident.

Id.

17. Notwithstanding its claim that it "takes the security of its patients' information very seriously," Sunrise has done nothing to mitigate the harm to its 427,000 patients.

B. Defendant's Privacy Practices

18. Sunrise maintains a series of privacy policies which discuss Sunrise's commitments regarding the protection of consumers' PII and PHI. The policies are contained in its Patient Privacy policy which states in relevant part:

> **We are Required to:**
>
> **Maintain the privacy and security of your health information**
> - Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sunrise is required by law to maintain the privacy of health information that identifies you, called protected health information or "PHI." Sunrise will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation.
>
> **Inform you if a breach occurs that may have compromised the privacy or security of your information**
> - Sunrise is required to provide patient notification if it discovers a breach of unsecured PHI unless there is a demonstration, based on a risk assessment, that there is a low probability that the PHI has been compromised. You will be notified without unreasonable delay and no later than 60 days after discovery of the breach.
>
> **Provide you with a notice of our legal duties and privacy practices regarding the information we collect and maintain about you**
> - Sunrise is required to provide you with this notice of our legal duties and privacy practices. A copy of our privacy practices is available on our website, www.sunriselab.com. You may also reDefendant that a printed copy be mailed to you (see below).

Abide by the terms of this notice

- Sunrise is required by law to maintain the privacy of your PHI and to abide by all of the terms of this notice.

Notify you by mail, upon your reDefendant, if Sunrise's health information practices change

- Sunrise may change the content of this notice of privacy practices at anytime because of operational or regulatory requirements. The changes will apply to all information Sunrise has about you. Whenever changes are made to this notice of privacy practices, they will be posted on Sunrise's website at www.sunriselab.com. If you reDefendant, you may be notified by mail whenever these changes occur. If you wish to have a copy of the changed notice of privacy practices mailed to you, contact Sunrise's Privacy Officer by calling 800.782.0282, Extension 1618 or email to **bgold@sunriselab.com**.

Obtain your written authorization for any uses or disclosures of your health information not described in this notice. You may revoke the authorization at any time, except to the extent that action has already been taken.

- For purposes not described above, Sunrise will ask for your authorization before using or disclosing your PHI. If you signed an authorization form, you may revoke it, in writing, at any time, except to the extent that Sunrise has already acted on any prior uses or disclosures previously authorized by you.[4]

19. The notice further states that "[w]e may provide your PHI to other companies or individuals that need the information to provide services to us. These other entities, known as 'business associates,' are required to maintain the privacy and security of PHI."[5]

20. Sunrise collects and stores an enormous amount of PII which it provides to its vendors and sub-contractors such as AMCA to further its business. As a recipient of sensitive patient PII, AMCA is similarly obligated to safeguard the integrity of such data on behalf of Sunrise patients.

21. Indeed, AMCA boldly states that it is "compliant with all Federal and State Laws and are members of ACA International. We provide our services adhering to the ethical guidelines expected from a National Accounts Receivable Management firm."[6]

[4] Available at https://www.sunriselab.com/patients/patient-privacy/ (last visited July 26, 2019).
[5] *Id*.

22. Consumers place value in data privacy and security, and they consider it when engaging services. Plaintiff and Class Members would not have utilized Sunrise's services had they known that Defendant did not take all necessary precautions to secure the personal data given to it by consumers.

23. Defendant failed to disclose its negligent and insufficient data security practices, and those of its subcontractors. Consumers relied on or otherwise were misled by this omission in deciding to use Defendant's services.

C. Defendant Was Aware That the Medical Industry was a Favorite Target of Hackers

24. The technology and medical industry are rife with similar examples of hackers targeting users' Private Information, including Anthem,[7] Premera,[8] and St. Joseph Health System[9] among others, all of which predate the time frame Sunrise and AMCA has identified regarding the Data Breach at issue in the present lawsuit.

25. Indeed, as early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or

[6] Available at http://amcaonline.com/about.php (last visited July 25, 2019).
[7] Los Angeles Times, *Anthem is warning consumers about its huge data breach. Here's a translation*, March 6, 2015. Available at http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html, last accessed July 25, 2019.
[8] New York Times, *Premera Blue Cross Says Data Breach Exposed Medical Data*, March 17, 2015. Available at http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0, last accessed July 25, 2019.
[9] Napa Valley Register, *St. Joseph Health System sued for patient data breach*, April 9, 2012. Available at http://napavalleyregister.com/news/local/st-joseph-health-system-sued-for-patient-data-breach/article_948c0896-82a3-11e1-bed6-0019bb2963f4.html, last accessed July 25, 2019.

Personally Identifiable Information (PII)."[10] Defendant's failure to heed this warning and to otherwise maintain adequate security practices resulted in this Data Breach.

D. The Value of Personally Identifiable Information

26. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[12] The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[13]

27. PII is such a valuable commodity that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[14] Indeed, as a result of large-scale data breaches, Social Security numbers, healthcare information, and other PII have been made publicly available to identity thieves and cyber criminals.

28. Professionals tasked with trying to stop fraud and other misuse acknowledge that PII has real monetary value in part because criminals continue their efforts to obtain this data.[15] According to the Identity Theft Resource Center, 2017 saw 1,579 data breaches, representing a 44.7

---

[10] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014. Available at http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820, last accessed July 25, 2019.
[11] 17 C.F.R § 248.201 (2013).
[12] *Id.*
[13] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide")(last visited July 25, 2019).
[14] FTC Guide, *supra* n.9.
[15] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, *CIO Magazine*, https://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited July 25, 2019).

percent increase over the record high figures reported a year earlier.[16] The Healthcare sector had the second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[17]

29. Healthcare related data is among the most sensitive, and personally consequential, when compromised. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[18] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[19]

30. Defendant knew the importance of safeguarding patient PII entrusted to them, and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on affected patients as a result of a breach.

E. Sunrise Acquires, Collects, and Stores Plaintiff's and Class Members' PII

31. Sunrise acquires, collects, stores, and maintains a massive amount of protected health related information and other personally identifiable information on their patients.

32. As a condition of engaging in health services, Sunrise requires that their customers entrust them with highly sensitive personal information.

---

[16] *2017 Annual Data Breach Year-End Review,* https://www.idtheftcenter.org/2017-data-breaches, (last visited January 23, 2019).
[17] Identity Theft Resource Center, 2018 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2018-data-breaches/ (last visited July 26, 2019).
[18] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited July 26, 2019)
[19] *Id.*

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII, Sunrise along with its vendors and sub-contractors assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members, as current and former patients, relied on the Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Sunrise acknowledges, as it must, its obligation to maintain the privacy of patient PII entrusted to them.

F. Defendant's Conduct Violates HIPAA and Industry Standard Practices

36. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

37. The Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;
b. Failing to mitigate the risks of a data breach and loss of data;
c. Failing to adequately catalog the location of Plaintiff's and Class Members' digital information;
d. Failing to properly encrypt Plaintiff's and Class Members' PII;
e. Failing to ensure the confidentiality and integrity of electronic protected health

information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

h. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

i. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

j. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94);

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*;

m. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

G. Defendant Failed to Maintain the Confidentiality of Plaintiff's and Class Members' Private Health Information

38. Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' PII.

39. Defendant's duties included ensuring Plaintiff's and Class Members' electronically protected PII was not made available or disclosed to unauthorized third persons or processes.

40. Defendant's duties also included protecting against reasonably anticipated threats or hazards to the security of Plaintiff's and Class Members' Private Health Information.

41. Defendant failed to adequately protect Plaintiff's and Class Members' PII from the reasonably anticipated threat of hackers accessing its systems and the PII contained therein.

42. As a result of Defendant's failure to protect against reasonably anticipated threats, Plaintiff and the Class Members' PII was improperly made available and disclosed to third persons.

43. Plaintiff and Class Members have a privacy right in their medical records, medical information, financial information and other PII.

44. As a result of Defendant's failure to maintain the confidentiality of Plaintiff and Class Members' PII, Plaintiff and Class Members suffered an injury through their loss of privacy.

H. Plaintiff and Class Members Suffered Damages

45. The ramifications of Defendant's failure to keep Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

46. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant.

47. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

48. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately invest in data security measures, despite its obligations to protect patient data.

49. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of PII.

50. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[20]

51. Despite professing to "taking the security of its patients' information very seriously," Sunrise has not offered patients anything to address the harm caused by them.

52. As a result of the Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and medical information being placed in the hands of criminals;

[20] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://-www.bjs.gov/content/pub/pdf/vit12.pdf (last visited July 25, 2019).

d. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

e. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in their possession; and

f. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

g. Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information and Private Health Information, for which there is a well-established national and international market;

h. Overpayments for products and services in that a portion of the price paid for such products and services by Plaintiff and Class Members was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which Defendant did not implement and, as a result, Plaintiff and Class Members did not receive what they paid for and were overcharged.

53. In addition to a remedy for economic harm suffered, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

54. Plaintiff seeks relief on behalf of herself and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII was exposed to unauthorized third parties as a result of the Data Breach announced on July 15, 2019 ("Class").[21]

[21] PII includes, but is not limited to, protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information including, without limitation to, names, health plan identification numbers, dates of birth, gender, address, health plan names, health plan eligibility dates, insurance types and coverage information.

55. Plaintiff also seeks certification of a New York Sub-Class defined as follows:

> All persons who reside in the State of New York whose PII was exposed to unauthorized third parties as a result of the Data Breach announced on July 15, 2019 ("New York Subclass").

56. Excluded from the Classes are Defendant and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

57. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

58. The proposed Classes meet the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

59. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of patients affected in the Data Breach is unknown, upon information and belief, it is approximately 427,000, and therefore meets the numerosity requirement of 23(a)(1).

60. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. Common questions include:

a. Whether Defendant had a duty to protect patient PII;

b. Whether Defendant knew or should have known of the susceptibility of their systems (and the systems of their contractors) to a data breach;

c. Whether Defendant's security measures to protect its systems were reasonable in light of the FTC data security recommendations, and best practices recommended by data security experts;

d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendant's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendant's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class Members are entitled to relief.

61. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a patient whose PII was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class Members', and Plaintiff seeks relief consistent with the relief sought by the Class.

62. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Classes she seeks to represent; is committed to pursuing this matter against Deendant to obtain relief for the Class; and has no conflict of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

63. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and

expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

64. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

65. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of FTC data security recommendations, and other best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

66. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purpose of providing notice.

FIRST CUASE OF ACTION
NEGLIGENCE

67. Plaintiff restates and realleges paragraphs 1 through 66 above as if fully set forth herein.

68. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Sunrise with their PII.

69. Plaintiff and the Class Members entrusted their PII to Sunrise with the understanding that Sunrise and its vendors and sub-contractors would safeguard their information.

70. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

71. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing the Defendant's security protocols to ensure that Plaintiff's and Class Members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cyber security measures regarding the security of patient information.

72. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the

inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

73. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

74. Plaintiff and the Class Members had no ability to protect their PII that was in Defendant's possession.

75. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

76. Defendant had a duty to have proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

77. Defendant has admitted that Plaintiff's and Class Members' PII was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

78. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII while it was within Defendant's possession or control and/or the possession or control of Defendant's vendors or subcontractors.

79. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

80. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII.

81. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

82. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

83. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

84. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to, out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud and the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

SECOND CAUSE OF ACTION
NEGLIGENT HIRING AND RETENTION

85. Plaintiff restates and realleges paragraphs 1 through 84 above as if fully set forth herein.

86. Defendant failed to exercise reasonable care in its hiring and retention practices to discover whether its third party vendors and/or employees were unfit, incompetent, unable, or unwilling to employ adequate security measures for consumer's PII which would create a risk of harm to others in the capacity for which those third party vendors and/or employees had been hired.

87. As a direct and proximate result of the aforesaid acts, omissions, negligence, carelessness, and/or recklessness of Defendant, Plaintiff and the Class were caused to suffer unlawful, extreme, and unreasonable invasions of their privacy, economic harms, and other damages including, but not limited to out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud and the costs associated therewith; time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY

88. Plaintiff restates and realleges paragraphs 1 through 87 above as if fully set forth herein.

89. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

90. Defendant owed a duty to patients, including Plaintiff and Class Members, to keep their PII confidential.

91. Defendant failed to protect patient PII by allowing unauthorized third parties to gain unfettered access to Plaintiff's and Class Members' PII.

92. The unauthorized release of PII, especially the type related to personal health information, is highly offensive to a reasonable person.

93. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their use of Sunrise's services, but privately with an intention that the PII would be kept confidential and would be

protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

94. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

95. Defendant acted with a knowing state of mind when it permitted the Data Breach because it was with actual knowledge that their information security practices were inadequate and insufficient.

96. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

97. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

98. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

FOURTH CAUSE OF ACTION
BREACH OF CONTRACT

99. Plaintiff restates and realleges paragraphs 1 through 98 above as if fully set forth herein.

100. Plaintiff and Class Members received medical services from Defendant, and in so doing provided their PII.

101. The contract for these services was supported by consideration in many forms including the payment of monies for medical services (e.g. laboratory testing services).

102. Plaintiff and Class Members performed pursuant to these contracts, and satisfied all conditions, covenants, obligations, and promises of the agreements.

103. Under these contracts, Defendant was obligated, as outlined in the Notice of Privacy Practices and Privacy Policy, to maintain the confidentiality of Plaintiff's and Class Member's PII.

104. Defendant's failure to maintain the confidentiality of Plaintiff and Class Members PII was a breach of Defendant's contractual obligations as outlined in their privacy practices.

105. Because Defendant failed to adequately secure Plaintiff and Class Member's PII, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between what was promised and what Defendant ultimately provided.

106. As a result of Defendant's breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PHI and PII and remain at imminent risk of suffering additional breaches in the future.

FIFTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

107. Plaintiff restates and realleges paragraphs 1 through 106 above as if fully set forth herein.

108. Plaintiff and Class Members were required to provide their PII, including names, addresses, dates of birth, social security numbers, credit card and bank information, among other

related information to as a condition of their use and or as a result of using and paying for Defendant's services.

109. Plaintiff and Class Members paid money to Defendant in exchange for services, implicit in which were Defendant's promises to protect patient PII from unauthorized disclosure.

110. In its written privacy policies, Defendant promised Plaintiff and Class Members that they would only disclose protected health information and other PII under certain circumstances, none of which relates to the Data Breach, and would otherwise comply with applicable state and federal laws.

111. Defendant promised and was otherwise obligated to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' protected health information and other PII would remain protected.

112. Implicit in Defendant's agreement with its patients, including Plaintiff and Class Members, to provide protected health information and other PII, and Defendant's acceptance of such protected health information and other PII, was Defendant's obligation to use the PII of patients for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

113. Further, implicit in the agreement, Defendant was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PII.

114. Without such implied contracts, Plaintiff and Class Members would not have provided their protected health information and other PII to Defendant.

115. Defendant had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

116. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

117. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

118. Defendant breached the implied contracts with Plaintiff and Class Members by:

a. failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach;

b. failing to comply with its obligations to abide by HIPAA;

c. failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);

d. failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii); and

g. failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

SIXTH CAUSE OF ACTION
UNJUST ENRICHMENT

119. Plaintiff restates and realleges paragraphs 1 through 118 above as if fully set forth herein.

120. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased medical services from Defendant and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and have their PII protected with adequate data security.

121. Defendant knew that Plaintiff and Class Members conferred a benefit on Defendant and accepted and have accepted or retained that benefit. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

122. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

123. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

124. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

125. Defendant acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

126. If Plaintiff and Class Members knew that Defendant would not secure their PII using adequate security measures, they would not have engaged in transactions with Defendant.

127. Plaintiff and Class Members have no adequate remedy at law.

128. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to (i) actual identity theft; (ii) the loss

of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of patients and in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendant's services they received.

129. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

130. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

SEVENTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

131. Plaintiff restates and realleges paragraphs 1 through 130 above as if fully set forth herein.

132. In light of the special relationship between Defendant and its Patients, whereby Defendant became guardians of Plaintiff's and Class Members' highly sensitive, confidential,

personal, financial information, and other PII, Defendant became a fiduciary created by its undertaking and guardianship of the PII, to act primarily for the benefit of its Patients, including Plaintiff and Class Members, for: 1) the safeguarding of Plaintiff and Class Members' PII; 2) timely notification of Plaintiff and Class Members of a data breach or disclosure; and 3) maintenance of complete and accurate records of what and where Defendant's patients' information was and is stored.

133. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their patients' relationship, in particular to keep secure the PII of their patients.

134. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' protected health information and other PII.

135. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

136. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

137. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

138. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

139. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

140. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

141. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

142. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94).

143. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, et seq.

144. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for

the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5).

145. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

146. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

147. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient PII in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendant's services they received.

148. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

EIGHTH CAUSE OF ACTION
BREACH OF CONFIDENCE

149. Plaintiff restates and realleges paragraphs 1 through 148 above as if fully set forth herein.

150. At all relevant times, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' protected health information and other PII that Plaintiff and Class Members provided to Defendant.

151. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' protected health information and other PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

152. Plaintiff and Class Members provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the protected health information and other PII to be disseminated to any unauthorized parties.

153. Plaintiff and Class Members also provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that protected health information and other PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

154. Defendant voluntarily received in confidence Plaintiff's and Class Members' protected health information and other PII with the understanding that protected health information and other PII would not be disclosed or disseminated to the public or any unauthorized third parties.

155. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' protected health information and other PII, Plaintiff's and Class Members' protected health information and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

156. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

157. But for Defendant's disclosure of Plaintiff's and Class Members' protected health information and other PII in violation of the parties' understanding of confidence, their protected health information and other PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected health information and other PII, as well as the resulting damages.

158. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' protected health information and other PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' protected health information and other PII had numerous security vulnerabilities because Defendant failed to observe even basic security practices necessary to prevent fraudulent provider accounts from being created.

159. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient PII in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendant's services they received.

160. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

NINTH CAUSE OF ACTION
VIOLATIONS OF THE INFORMATION SECURITY BREACH AND NOTIFICATION ACT, N.Y. Gen. Bus. Law § 899-aa

161. Plaintiff restates and realleges Paragraphs 1 through 160 as if fully set forth here.

162. Plaintiff brings this cause of action on behalf of herself and the New York Subclass.

163. Sunrise is a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law. § 899-aa(1)(a). Sunrise also maintains computerized

data that includes Personal Information that Sunrise does not own. Accordingly, it is subject to N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

164. Plaintiff and New York Subclass members' PII includes Personal Information covered by N.Y. Gen. Bus. Law § 899-aa(a)(b).

165. Sunrise is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Sunrise does not own, including Plaintiff and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

166. Sunrise is required to accurately notify Plaintiff and New York Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Sunrise owns or licenses, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

167. By failing to disclose the Sunrise data breach in a timely and accurate manner, Sunrise violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

168. As a direct and proximate result of Sunrise's violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass members suffered damages, as described above.

169. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing Defendant to hereinafter adequately safeguard the Class' PII by implementing improved security procedures and measures;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

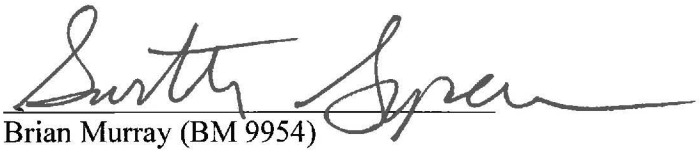
h. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues so triable by a jury.

Dated: July 30, 2019

GLANCY PRONGAY & MURRAY LLP



Brian Murray (BM 9954)
Brian D. Brooks
Garth Spencer
230 Park Avenue, Suite 530
New York, NY 10169
Telephone: (212) 682-5340
Facsimile: (212) 884-0988
bmurray@glancylaw.com
bbrooks@glancylaw.com
gspencer@glancylaw.com

JONES WARD PLC
Jasper D. Ward
Marion E. Taylor Building
312 South Fourth Street, Sixth Floor
Louisville, Kentucky 40202
Telephone: (502) 882-6000
Facsimile: (502) 587-2007
jasper@jonesward.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@forthepeople.com

Counsel for Plaintiffs